

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-149061

(P2002-149061A)

(43) 公開日 平成14年5月22日 (2002.5.22)

| (51) Int.Cl. ¹ | 識別記号 | F I | テーマコード(参考) |
|--------------------------------------|-------|---------------|-------------------|
| G 0 9 C 1/00 | 6 4 0 | G 0 9 C 1/00 | 6 4 0 B 5 B 0 1 7 |
| | 6 6 0 | | 6 4 0 Z 5 B 0 3 5 |
| G 0 6 F 12/00 | 5 3 7 | G 0 6 F 12/00 | 6 6 0 A 5 B 0 4 9 |
| 12/14 | 3 2 0 | 12/14 | 5 3 7 H 5 B 0 5 8 |
| | | | 3 2 0 F 5 B 0 8 2 |
| 審査請求 未請求 請求項の数10 O L (全 26 頁) 最終頁に続く | | | |

(21) 出願番号 特願2000-348531(P2000-348531)

(22) 出願日 平成12年11月15日 (2000. 11. 15)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 太田 貢太郎

東京都港区芝五丁目7番1号 日本電気株式会社内

(72) 発明者 添田 修材

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100065385

弁理士 山下 稯平

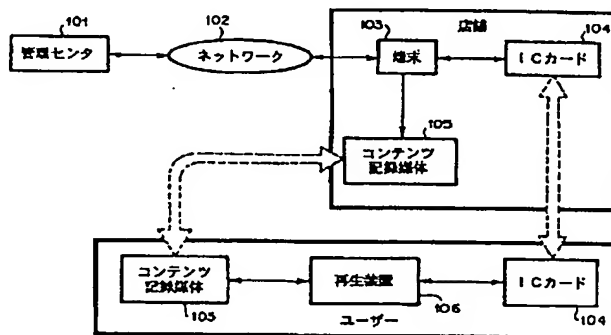
最終頁に続く

(54) 【発明の名称】 レンタルコンテンツ流通システムおよびその方法

(57) 【要約】

【課題】 デジタルコンテンツの流通において、ユーザの利便性の向上と店舗の利益損失の解消と安全なコンテンツ保護を行う流通システムと流通方法を提供する。

【解決手段】 再生装置106とICカードが相互認証し、ICカードと管理センタ101が相互認証し、ICカードは再生装置から受信した再生装置公開鍵証明書を送信し、管理センタに送信し、端末がコンテンツタイトルとレンタル期間を含む契約情報を使用者から入力し、これにICカードによる署名を付したものを管理センタが受信し、管理センタがコンテンツ暗号鍵等を再生装置公開鍵等で暗号化して、署名して端末に送り、端末はそれをICカードに書き込み、署名照合結果が正しければ、端末がコンテンツを記録媒体105に記録し、再生装置106は、ICカードから受信する暗号化されたコンテンツ暗号鍵を復号し、それを用いてコンテンツを復号する。



【特許請求の範囲】

【請求項1】 再生装置公開鍵を含む再生装置公開鍵証明書を送信し、ICカード公開鍵を前記ICカードから前記再生装置へ送信しつつ行われる、前記再生装置と前記ICカードの間で相互認証を行うステップと、

ICカード公開鍵を含むICカード公開鍵証明書を前記ICカードから管理センタへ送信しつつ行われる、前記ICカードと管理センタとの間で端末を介して相互認証を行うステップと、

前記端末を介して前記ICカードから前記再生装置公開鍵証明書を前記管理センタへ送信するステップと、

前記管理センタが、前記再生装置公開鍵証明書を認証するステップと、

前記端末が、契約情報を操作者から入力するステップと、

前記端末が、契約情報を前記ICカードに送信するステップと、

前記ICカードが、前記契約情報にICカード秘密鍵により署名を付するステップと、

前記ICカードが、前記ICカード秘密鍵により署名が付された前記契約情報を前記端末を介して前記管理センタに送信するステップと、

前記管理センタが、前記契約情報を、前記契約情報に前記ICカード秘密鍵により付された署名と照合するステップと、

前記管理センタが、前記契約情報中にあるコンテンツタイトルに対応するコンテンツ暗号鍵に管理センタ秘密鍵により署名を付するステップと、

前記管理センタが、前記管理センタ秘密鍵により署名が付された前記コンテンツ暗号鍵を前記再生装置公開鍵証明書中の再生装置公開鍵により暗号化するステップと、

前記管理センタが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により署名を付するステップと、

前記管理センタが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ICカード公開鍵により暗号化するステップと、

前記管理センタが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ICカード公開鍵により暗号化されたこれらのものを前記端末

を介して前記ICカードに送信するステップと、

前記ICカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ICカード公開鍵により暗号化されたこれらのものより、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ICカード秘密鍵により復号するステップと、

前記ICカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合するステップと、

前記ICカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵を記憶するステップと、

前記ICカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合する前記ステップの結果が正常であるときに、正常終了の旨を前記端末に送信するステップと、

前記端末が、前記正常終了の旨を前記ICカードから受信したときに、前記コンテンツタイトルに対応するコンテンツデータであって前記コンテンツ暗号鍵により暗号化されているものを記録媒体に記録するステップと、

前記再生装置が、前記ICカードに前記コンテンツ暗号鍵の要求を送信するステップと、

前記ICカードが、前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ICカード秘密鍵により署名を付するステップと、

前記ICカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ICカード秘密鍵により付された署名を前記再生装置に送信するステップと、

前記再生装置が、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名と照合するステップと、

前記再生装置が、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵より、前記コンテンツ暗号鍵及び前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名を再生装置秘密鍵により復号するステップと、

前記再生装置が、前記コンテンツ暗号鍵を、前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名と照合するステップと、

前記再生装置が、前記コンテンツ暗号鍵を記憶するステップと、

前記再生装置が、前記記録媒体に記録されている暗号化されている前記コンテンツデータより前記コンテンツ暗号鍵によりコンテンツデータを復号するステップと、を有することを特徴とするレンタルコンテンツ流通方法。

【請求項２】 請求項１に記載のレンタルコンテンツ流通方法において、前記契約情報には契約期間が含まれ、前記ＩＣカードが、前記契約情報中の契約期限を前記ＩＣカードのタイマにセットするステップと、

前記ＩＣカードが、前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記ＩＣカードのタイマからタイマ値を読み出すステップと、

を有し、

前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付する代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により署名を付し、

前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記ＩＣカードのタイマから読み出されたタイマ値及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信し、

前記再生装置が、前記再生装置のタイマに受信したタイ

マ値をセットするステップと、

前記ＩＣカードが、前記ＩＣカードのタイマの値が所定値になると、前記ＩＣカードが記憶する前記コンテンツ暗号鍵を消去するステップと、

前記再生装置が、前記再生装置のタイマの値が所定値になると、前記再生装置が記憶する前記コンテンツ暗号鍵を消去するステップと、

を有することを特徴とするレンタルコンテンツ流通方法。

【請求項３】 再生装置公開鍵を含む再生装置公開鍵証明書を再生装置からＩＣカードへ送信し、ＩＣカード公開鍵を前記ＩＣカードから受信しつつ、前記ＩＣカードの間で相互認証を行う手段と、

前記ＩＣカードにコンテンツ暗号鍵の要求を送信する手段と、

管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化されたコンテンツ暗号鍵を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵にＩＣカード秘密鍵により付された署名と照合する手段と、

前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵より、前記コンテンツ暗号鍵及び前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名を再生装置秘密鍵により復号する手段と、

前記コンテンツ暗号鍵を、前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名と照合する手段と、

前記コンテンツ暗号鍵を記憶する手段と、

記録媒体に記録されている暗号化されている前記コンテンツデータより前記コンテンツ暗号鍵によりコンテンツデータを復号する手段と、

を備えることを特徴とする再生装置。

【請求項４】 請求項３に記載の再生装置において、

前記契約情報には契約期間が含まれ、

受信したタイマ値が設置されるタイマと、

前記タイマの値が所定値になると、記憶する前記コンテンツ暗号鍵を消去する手段と、

を備えることを特徴とする再生装置。

【請求項５】 再生装置公開鍵を含む再生装置公開鍵証明書を再生装置から受信し、ＩＣカード公開鍵を前記再生装置へ送信しつつ、前記再生装置との間で相互認証を行う手段と、

ＩＣカード公開鍵を含むＩＣカード公開鍵証明書を管理センタへ送信しつつ、管理センタとの間で端末を介して相互認証を行う手段と、

前記端末を介して前記再生装置公開鍵証明書を前記管理センタへ送信する手段と、

前記端末から契約情報を受信する手段と、

前記契約情報にＩＣカード秘密鍵により署名を付する手

段と、

前記ＩＣカード秘密鍵により署名が付された前記契約情報を前記端末を介して前記管理センタに送信する手段と、

管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化されたコンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものを前記端末を介して前記管理センタから受信する手段と、

前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものより、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード秘密鍵により復号する手段と、

前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合する手段と、

前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵を記憶する手段と、

前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合する前記ステップの結果が正常であるときに、正常終了の旨を前記端末に送信する手段と、

前記再生装置から前記コンテンツ暗号鍵の要求を受信する手段と、

前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付する手段と、

前記管理センタ秘密鍵により署名が付され前記再生装置

公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する手段と、

を備えることを特徴とするＩＣカード。

【請求項６】 請求項５に記載のＩＣカードにおいて、前記契約情報には契約期間が含まれ、前記契約情報中の契約期限がセットされるタイマと、前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記タイマからタイマ値を読み出す手段と、前記タイマの値が所定値になると、記憶する前記コンテンツ暗号鍵を消去する手段と、

を備え、

前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付する手段の代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により署名を付する手段を備え、

前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する手段の代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記ＩＣカードのタイマから読み出されたタイマ値及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する手段を備えることを特徴とするＩＣカード。

【請求項７】 ＩＣカード公開鍵を含むＩＣカード公開鍵証明書をＩＣカードから管理センタへ送信しつつ行われる前記ＩＣカードと管理センタとの間での相互認証に仲介する手段と、

前記ＩＣカードから前記管理センタへの前記再生装置公開鍵証明書の送信を仲介する手段と、

契約情報を操作者から入力する手段と、

前記契約情報を前記ＩＣカードに送信する手段と、

前記ＩＣカードから前記管理センタへのＩＣカード秘密鍵により署名が付された前記契約情報の送信を仲介する手段と、

前記管理センタから前記ＩＣカードへの管理センタ秘密鍵により署名が付され再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵に

より暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものの送信を仲介する手段と、

前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合した結果が正常であるときに、正常終了の旨を前記ＩＣカードから受信する手段と、前記正常終了の旨を前記ＩＣカードから受信したときに、前記コンテンツタイトルに対応するコンテンツデータであって前記コンテンツ暗号鍵により暗号化されているものを記録媒体に記録する手段と、を備えることを特徴とする端末。

【請求項８】 ＩＣカード公開鍵を含むＩＣカード公開鍵証明書を含むＩＣカードから受信しつつ、前記ＩＣカードとの間で端末を介して相互認証を行う手段と、前記端末を介して前記ＩＣカードから再生装置公開鍵を含む再生装置公開鍵証明書を受信する手段と、前記再生装置公開鍵証明書を認証する手段と、前記ＩＣカードからＩＣカード秘密鍵により署名が付された契約情報を前記端末を介して受信する手段と、前記契約情報を、前記契約情報に前記ＩＣカード秘密鍵により付された署名と照合する手段と、前記契約情報中にあるコンテンツタイトルに対応するコンテンツ暗号鍵に管理センタ秘密鍵により署名を付する手段と、前記管理センタ秘密鍵により署名が付された前記コンテンツ暗号鍵を前記再生装置公開鍵証明書中の再生装置公開鍵により暗号化する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード公開鍵により暗号化する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものを前記端末を介して前記ＩＣカ

ードに送信する手段と、を備えることを特徴とする管理センタ。

【請求項９】 請求項３に記載の再生装置と、請求項５に記載のＩＣカードと、請求項７に記載の端末と、請求項８に記載の管理センタを備えることを特徴とするレンタルコンテンツ流通システム。

【請求項１０】 請求項４に記載の再生装置と、請求項６に記載のＩＣカードと、請求項７に記載の端末と、請求項８に記載の管理センタを備えることを特徴とするレンタルコンテンツ流通システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、再生装置、再生情報記憶装置、管理センタ、コンテンツ流通システムにおいて、コンテンツ再生期限の管理、コンテンツを再生する再生装置の限定方法、コンテンツを再生する再生装置の機種の安全な変更方法に関する。

【０００２】

【従来の技術】第１の従来技術として、デジタルコンテンツのレンタルはビデオテープと同様にＤＶＤやＣＤを貸与しレンタル期間内に返却する方式がある。

【０００３】第２の従来技術として、ＤＶＤにはコンテンツの不正コピーを防止するためコンテンツデータを暗号化し媒体に記録され、暗号化したコンテンツデータを復号する鍵データも媒体に記録されている。

【０００４】第３の従来技術として、ＤＶＤ媒体へは暗号化されたコンテンツデータを記録し、復号する鍵データは電話回線等からインターネットを介して再生装置にダウンロードするには方式がある。

【０００５】

【発明が解決しようとする課題】しかしながら、この第１の従来技術による方法では、レンタルしたＤＶＤやＣＤをレンタル期間内に店舗に赴き返却しなければならず大変煩わしかった。

【０００６】また、レンタル期間を誤って超過しても追加料金を徴収されていた。

【０００７】さらに、レンタルした本人以外がコンテンツを再生するいわゆる見回し行為によってレンタル店に損失を与えていた。

【０００８】第２の従来技術による方法では、媒体には暗号化されたコンテンツデータを復号する鍵データを記録されているため、ハッカーによる不正な暗号の解読行為を防止することは不可能であり常に解読される脅威にさらされる。

【０００９】また昨今、ＤＶＤのライセンスを受けた企業であっても不手際により機密が漏洩し、暗号データが解読されており、機密情報の管理方法に問題があった。

【００１０】第３の従来技術による方法では、コンテンツ再生のためにユーザがプロバイダ契約や接続のための難解な設定を行う必要があり煩雑であった。

【0011】本発明は、上記従来の問題点を鑑みなされたものであり、デジタルコンテンツの流通において、ユーザの利便性の向上と店舗の利益損失の解消と安全なコンテンツ保護を行う流通システムと流通方法を提供することを目的とする。

【0012】

【課題を解決するための手段】本発明によるレンタルコンテンツ流通方法は、再生装置公開鍵を含む再生装置公開鍵証明書を再生装置からＩＣカードへ送信し、ＩＣカード公開鍵を前記ＩＣカードから前記再生装置へ送信しつつ行われる、前記再生装置と前記ＩＣカードの間で相互認証を行うステップと、ＩＣカード公開鍵を含むＩＣカード公開鍵証明書を前記ＩＣカードから管理センタへ送信しつつ行われる、前記ＩＣカードと管理センタとの間で端末を介して相互認証を行うステップと、前記端末を介して前記ＩＣカードから前記再生装置公開鍵証明書を前記管理センタへ送信するステップと、前記管理センタが、前記再生装置公開鍵証明書を認証するステップと、前記端末が、契約情報を操作者から入力するステップと、前記端末が、契約情報を前記ＩＣカードに送信するステップと、前記ＩＣカードが、前記契約情報にＩＣカード秘密鍵により署名を付するステップと、前記ＩＣカードが、前記ＩＣカード秘密鍵により署名が付された前記契約情報を前記端末を介して前記管理センタに送信するステップと、前記管理センタが、前記契約情報を、前記契約情報に前記ＩＣカード秘密鍵により付された署名と照合するステップと、前記管理センタが、前記契約情報中にあるコンテンツタイトルに対応するコンテンツ暗号鍵に管理センタ秘密鍵により署名を付するステップと、前記管理センタが、前記管理センタ秘密鍵により署名が付された前記コンテンツ暗号鍵を前記再生装置公開鍵証明書中の再生装置公開鍵により暗号化するステップと、前記管理センタが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により署名を付するステップと、前記管理センタが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード公開鍵により暗号化するステップと、前記管理センタが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものを前記端末を介して前記ＩＣカードに送信する

ステップと、前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものより、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード秘密鍵により復号するステップと、前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合するステップと、前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵を記憶するステップと、前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合する前記ステップの結果が正常であるときに、正常終了の旨を前記端末に送信するステップと、前記端末が、前記正常終了の旨を前記ＩＣカードから受信したときに、前記コンテンツタイトルに対応するコンテンツデータであって前記コンテンツ暗号鍵により暗号化されているものを記録媒体に記録するステップと、前記再生装置が、前記ＩＣカードに前記コンテンツ暗号鍵の要求を送信するステップと、前記ＩＣカードが、前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付するステップと、前記ＩＣカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信するステップと、前記再生装置が、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵に

より付された署名と照合するステップと、前記再生装置が、前記管理センタ秘密鍵により名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵より、前記コンテンツ暗号鍵及び前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名を再生装置秘密鍵により復号するステップと、前記再生装置が、前記コンテンツ暗号鍵を、前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名と照合するステップと、前記再生装置が、前記コンテンツ暗号鍵を記憶するステップと、前記再生装置が、前記記録媒体に記録されている暗号化されている前記コンテンツデータより前記コンテンツ暗号鍵によりコンテンツデータを復号するステップと、を有することを特徴とする。

【0013】上記のレンタルコンテンツにおいて、前記契約情報には契約期間が含まれ、前記ICカードが、前記契約情報中の契約期限を前記ICカードのタイマにセットするステップと、前記ICカードが、前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記ICカードのタイマからタイマ値を読み出すステップと、を有し、前記ICカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ICカード秘密鍵により署名を付する代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ICカードのタイマから読み出されたタイマ値に前記ICカード秘密鍵により署名を付し、前記ICカードが、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ICカード秘密鍵により付された署名を前記再生装置に送信する代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記ICカードのタイマから読み出されたタイマ値及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ICカードのタイマから読み出されたタイマ値に前記ICカード秘密鍵により付された署名を前記再生装置に送信し、前記再生装置が、前記再生装置のタイマに受信したタイマ値をセットするステップと、前記ICカードが、前記ICカードのタイマの値が所定値になると、前記ICカードが記憶する前記コンテンツ暗号鍵を消去するステップと、前記再生装置が、前記再生装置のタイマの値が所定値になると、前記再生装置が記憶する前記コンテンツ暗号鍵を消去するステップと、を有していてもよい。

【0014】本発明による再生装置は、再生装置公開鍵を含む再生装置公開鍵証明書を再生装置からICカードへ送信し、ICカード公開鍵を前記ICカードから受信しつつ、前記ICカードの間で相互認証を行う手段と、

前記ICカードにコンテンツ暗号鍵の要求を送信する手段と、管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化されたコンテンツ暗号鍵を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵にICカード秘密鍵により付された署名と照合する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵より、前記コンテンツ暗号鍵及び前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名を再生装置秘密鍵により復号する手段と、前記コンテンツ暗号鍵を、前記コンテンツ暗号鍵に付された前記管理センタ秘密鍵による署名と照合する手段と、前記コンテンツ暗号鍵を記憶する手段と、記録媒体に記録されている暗号化されている前記コンテンツデータより前記コンテンツ暗号鍵によりコンテンツデータを復号する手段と、を備えることを特徴とする。

【0015】上記の再生装置において、前記契約情報には契約期間が含まれ、受信したタイマ値が設置されるタイマと、前記タイマの値が所定値になると、記憶する前記コンテンツ暗号鍵を消去する手段と、を備えていてもよい。

【0016】本発明によるICカードは、再生装置公開鍵を含む再生装置公開鍵証明書を再生装置から受信し、ICカード公開鍵を前記再生装置へ送信しつつ、前記再生装置との間で相互認証を行う手段と、ICカード公開鍵を含むICカード公開鍵証明書を管理センタへ送信しつつ、管理センタとの間で端末を介して相互認証を行う手段と、前記端末を介して前記再生装置公開鍵証明書を前記管理センタへ送信する手段と、前記端末から契約情報を受信する手段と、前記契約情報にICカード秘密鍵により署名を付する手段と、前記ICカード秘密鍵により署名が付された前記契約情報を前記端末を介して前記管理センタに送信する手段と、管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化されたコンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ICカード公開鍵により暗号化されたこれらのものを前記端末を介して前記管理センタから受信する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ICカード公開鍵により暗号化されたこれらのものより、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ

秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード秘密鍵により復号する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵を記憶する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合する前記ステップの結果が正常であるときに、正常終了の旨を前記端末に送信する手段と、前記再生装置から前記コンテンツ暗号鍵の要求を受信する手段と、前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する手段と、を備えることを特徴とする。

【００１７】上記のＩＣカードにおいて、前記契約情報には契約期間が含まれ、前記契約情報中の契約期限がセットされるタイマと、前記再生装置から前記コンテンツ暗号鍵の要求を受信したときに、前記タイマからタイマ値を読み出す手段と、前記タイマの値が所定値になると、記憶する前記コンテンツ暗号鍵を消去する手段と、を備え、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により署名を付する手段の代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により署名を付する手段を備え、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する手段の代わりに、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記

コンテンツ暗号鍵、前記ＩＣカードのタイマから読み出されたタイマ値及び管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記ＩＣカードのタイマから読み出されたタイマ値に前記ＩＣカード秘密鍵により付された署名を前記再生装置に送信する手段を備えていてもよい。

【００１８】本発明による端末は、ＩＣカード公開鍵を含むＩＣカード公開鍵証明書を含むＩＣカードから管理センタへ送信しつつ行われる前記ＩＣカードと管理センタとの間での相互認証に仲介する手段と、前記ＩＣカードから前記管理センタへの前記再生装置公開鍵証明書の送信を仲介する手段と、契約情報を操作者から入力する手段と、前記契約情報を前記ＩＣカードに送信する手段と、前記ＩＣカードから前記管理センタへのＩＣカード秘密鍵により署名が付された前記契約情報の送信を仲介する手段と、前記管理センタから前記ＩＣカードへの管理センタ秘密鍵により署名が付され再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものの送信を仲介する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報を、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名と照合した結果が正常であるときに、正常終了の旨を前記ＩＣカードから受信する手段と、前記正常終了の旨を前記ＩＣカードから受信したときに、前記コンテンツタイトルに対応するコンテンツデータであって前記コンテンツ暗号鍵により暗号化されているものを記録媒体に記録する手段と、を備えることを特徴とする。

【００１９】本発明による管理センタは、ＩＣカード公開鍵を含むＩＣカード公開鍵証明書をＩＣカードから受信しつつ、前記ＩＣカードとの間で端末を介して相互認証を行う手段と、前記端末を介して前記ＩＣカードから再生装置公開鍵を含む再生装置公開鍵証明書を受信する手段と、前記再生装置公開鍵証明書を認証する手段と、前記ＩＣカードからＩＣカード秘密鍵により署名が付された契約情報を前記端末を介して受信する手段と、前記契約情報を、前記契約情報に前記ＩＣカード秘密鍵により付された署名と照合する手段と、前記契約情報中にあるコンテンツタイトルに対応するコンテンツ暗号鍵に管理センタ秘密鍵により署名を付する手段と、前記管理センタ秘密鍵により署名が付された前記コンテンツ暗号鍵を前記再生装置公開鍵証明書中の再生装置公開鍵により暗号化する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コン

テンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により署名を付する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名を前記ＩＣカード公開鍵により暗号化する手段と、前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵、前記契約情報並びに前記管理センタ秘密鍵により署名が付され前記再生装置公開鍵により暗号化された前記コンテンツ暗号鍵及び前記契約情報に前記管理センタ秘密鍵により付された署名であって前記ＩＣカード公開鍵により暗号化されたこれらのものを前記端末を介して前記ＩＣカードに送信する手段と、を備えることを特徴とする。

【００２０】本発明によるレンタルコンテンツ流通システムは、上記の再生装置と、上記のＩＣカードと、上記の端末と、上記の管理センタを備えることを特徴とする。

【００２１】

【発明の実施の形態】本発明の上記および他の目的、特徴および利点を明確にすべく、以下添付した図面を参照しながら、本発明の実施の形態につき詳細に説明する。

【００２２】図１を参照すると、本発明の一実施の形態としてのレンタルコンテンツ流通におけるシステムおよび流通方法の構成例が示されている。

【００２３】図１において、レンタルコンテンツ流通システムは、管理センタ１０１と、店舗に設置した端末１０３と、管理センタ１０１と端末１０３を結ぶネットワーク１０２と、ＩＣカード１０４とコンテンツ記録媒体１０５と、ユーザに設置されている再生装置１０６から構成される。

【００２４】図１において、管理センタ１０１は遠隔地に設置され、インターネット等のネットワーク１０２を介して店舗に設置している端末１０３と接続されている。なお図では省略しているが店舗は複数存在し、また１店舗に端末１０３が複数あっても良い。

【００２５】端末１０３にはユーザが持参したＩＣカード１０４とコンテンツ記録媒体１０５を接続する。

【００２６】再生装置１０６はユーザが所有しており、ユーザが所有しているＩＣカード１０４とコンテンツ記録媒体１０５を接続する。

【００２７】管理センタ１０１は複数のコンテンツ暗号鍵と、全ＩＣカードの公開鍵証明書と、全再生装置の公開鍵証明書と全ＩＣカードと全再生装置のペア情報を保管しており、端末１０３を介してＩＣカード１０４からＩＣカードの公開鍵証明書と再生装置の公開鍵証明書を受信し正当性を確認する。コンテンツ暗号鍵は、コンテンツ毎に異なり、それぞれのコンテンツ暗号鍵によりそ

れぞれのコンテンツが暗号化される。

【００２８】また端末１０３を介してＩＣカード１０４と相互認証した後、端末からの所定の手続きによりコンテンツ暗号鍵とレンタル期間情報をＩＣカード１０４へ配信する。

【００２９】端末１０３には管理センタ１０１で保管しているコンテンツ暗号鍵で暗号化されたコンテンツが記録されており、ユーザは端末１０３によってコンテンツをレンタル購入するための操作を行う。

【００３０】端末１０３は管理センタ１０１とＩＣカード１０４との所定の手続きにより、コンテンツ記録媒体１０５に暗号化されたコンテンツをダウンロードする。

【００３１】ＩＣカード１０４は端末１０３を介して、コンテンツを暗号化したコンテンツ暗号鍵とレンタル期限情報をダウンロードし、レンタル期間中コンテンツ暗号鍵を保管し、レンタル期間を過ぎるとコンテンツ暗号鍵を消去する。

【００３２】また、ＩＣカードはユーザが所有している再生装置１０６との間で相互認証を行い、所定の手続きによりレンタル期間中はコンテンツ暗号鍵を再生装置１０６に配信する。

【００３３】コンテンツ記録媒体１０５は、管理センタ１０１とＩＣカード１０４の所定の手続きにより端末１０３に記録された暗号化されているコンテンツを記録する。また、コンテンツ記録媒体１０５はユーザが所有する再生装置１０６へ所定の手続き後、再生装置１０６の制御によりコンテンツデータが読み出される。

【００３４】ユーザが所有している再生装置１０６は、ＩＣカード１０４との認証処理後の所定の手続きによりＩＣカード１０４から送信されたコンテンツ暗号鍵をレンタル期間中まで保管し、レンタル期間が過ぎるかあるいは電源が切断されるまで保持する。

【００３５】また、再生装置１０６はコンテンツ記憶媒体１０５から暗号化されたコンテンツを所定の手続きにより読み出し、暗号化されたコンテンツデータをＩＣカード１０４から読み出したコンテンツ暗号鍵によって復号しレンタル期間中はコンテンツを再生する。

【００３６】図１の例の場合、順をおって説明する。

【００３７】まずＩＣカード１０１は前もって再生装置１０６と接続し、ＩＣカード１０４と再生装置１０６との間で相互認証を行う。ＩＣカード１０４は、相互認証の結果が正常であれば、再生装置公開鍵の証明書を記憶する。

【００３８】次にユーザはＩＣカード１０４とコンテンツ記録媒体１０５を店舗へ持参し端末１０３に接続する。

【００３９】端末１０３はＩＣカード１０４が接続されるとＩＣカード１０４からＩＣカード１０４の公開鍵証明書を読み出し、管理センタ１０１へ読み出したＩＣカード１０４の公開鍵証明書と共に相互認証の要求を行

う。

【0040】管理センタ101はICカード104の公開鍵証明書の有効性を確認し、ICカード104との間で相互認証を行う。

【0041】次に端末103は再生装置106の公開鍵証明書を読み出し、管理センタ101へ読み出した再生装置106の公開鍵証明書を転送する。

【0042】管理センタ101は再生装置106の公開鍵証明書の有効性を確認する。

【0043】次にユーザは端末103へレンタルするコンテンツのタイトルとレンタル期間を入力すると、端末103はICカードへコンテンツのタイトルとレンタル期間を含む契約情報を送信し、ICカード104から契約情報と契約情報へのICカードの秘密鍵による署名を読み出す。

【0044】端末103は管理センタ101に対してコンテンツ暗号鍵を要求するデータとして契約情報と契約情報への署名データを送信する。

【0045】次に管理センタ101は、端末103からの契約情報と契約情報への署名を検証してデータの正当性が確認された場合、コンテンツタイトルに対応するコンテンツ暗号鍵を再生装置106の公開鍵を用いて暗号化し、その暗号化されたコンテンツ暗号鍵等とコンテンツ暗号鍵等への管理センターの秘密鍵による署名データをICカード104へ端末103を介して送信する。

【0046】ICカード104は再生装置106の公開鍵によって暗号化されたコンテンツ暗号鍵と署名データを検証し、正当性が確認された場合、再生装置106の公開鍵によって暗号化されたコンテンツ暗号鍵をレンタル期間中のみ保管する。

【0047】次に、端末103は、コンテンツタイトルに対応するコンテンツ暗号鍵によって既に暗号化されているコンテンツを所定の手順によりコンテンツ記録媒体105に転送し、ユーザは店舗にレンタル料金を支払い後、ICカード104とコンテンツ記録媒体105を受け取る。

【0048】次にユーザは所有の再生装置106へICカード104とコンテンツ記録媒体105を接続する。

【0049】再生装置106はICカード104との間で相互認証し、正当性が確認できるとICカード104からコンテンツ暗号鍵とコンテンツ暗号鍵への署名と契約情報等及び契約情報等への署名を読み取る。

【0050】再生装置106はコンテンツ暗号鍵、契約情報と署名データを照合しデータの正当性が確認されると、再生装置106の公開鍵によって暗号化されているコンテンツ暗号鍵を再生装置106の秘密鍵で復号し、復号されたコンテンツ暗号鍵をレンタル期間あるいは電源が切断されるまで保管する。

【0051】再生装置106はコンテンツ記憶媒体105から暗号されたコンテンツを読み出し、コンテンツ暗

号鍵で復号しレンタル期間中あるいは電源が切断されるまでコンテンツを再生する。

【0052】図2を参照すると、図1に示す管理センタ101の詳細な構成例が示されている。

【0053】管理センタは制御部201、復号部202、暗号部203、圧縮部204、乱数発生部205、認証部206、通信部207、管理センタ秘密鍵記憶部208、管理センタ公開鍵記憶部209、コンテンツ暗号鍵記憶部210、公開鍵データベース211、課金情報データベース212を備える。

【0054】管理センタ秘密鍵記憶部208には管理センタ101のみが所有する管理センタ秘密鍵が記録されている。

【0055】管理センタ公開鍵記憶部209には管理センタ秘密鍵と所定の方法によりペアとなる管理センタ公開鍵が記録されている。

【0056】コンテンツ暗号鍵記憶部210には、各コンテンツを暗号化するために用いられた各コンテンツ暗号鍵が記憶されている。各コンテンツ暗号鍵は、共通鍵である。

【0057】公開鍵データベース211には、全ICカードと全再生装置の公開鍵証明書と全ICカードと全再生装置のペア情報（秘密鍵と公開鍵より成る情報）が記録されている。

【0058】課金情報データベース212には、ユーザがレンタルしたコンテンツについてのタイトルとレンタル期間とレンタル料金が記録されている。

【0059】復号部202は通信部207を介して店舗の端末103からの暗号化データを受信すると制御部101の制御により、管理センタ秘密鍵記憶部208に記憶されている管理センタ秘密鍵、あるいは公開鍵データベース210に記録されたICカードの公開鍵や再生装置の公開鍵を使って暗号データを復号する。

【0060】暗号部203は、通信部207を介して店舗の端末103へデータを送信する時、制御部201の制御で管理センタ秘密鍵記憶部208に記憶している管理センタ秘密鍵あるいは公開鍵データベースに記録されたICカードの公開鍵や再生装置の公開鍵を使いデータを暗号化する。

【0061】圧縮部204はハッシュ関数を用いて制御部201の制御により任意のデータの圧縮を行う。

【0062】乱数発生部205は制御部201の制御により乱数を発生する。

【0063】認証部206は相互認証時に送信した乱数と受信した乱数の照合と、受信したデータと署名データの照合を行う。

【0064】図3を参照すると、図1に示す端末103の詳細な構成例が示されている。

【0065】端末103は、制御部301、通信部302、ICカード入出力部303、コンテンツ記録媒体出

力部304、入力部305、表示部306、コンテンツ記憶部307から構成されている。

【0066】通信部302は制御部301の制御によりインターネット等のネットワーク102を介して管理センタ101と通信を行う。

【0067】ICカード入出力部303は制御部301の制御によりICカード104と通信する。

【0068】コンテンツ記録媒体出力部304は制御部301の制御によりコンテンツ記録媒体105へコンテンツ記憶部307のコンテンツデータを出力する。

【0069】入力部305はレンタルするコンテンツの選択とレンタル期間をユーザが操作し入力するためのユーザインターフェースである。

【0070】表示部306はレンタルするコンテンツのタイトル表示とレンタル期間を表示するユーザインターフェースである。

【0071】コンテンツ記憶部307には、暗号化されたコンテンツが記憶されている。

【0072】図4を参照すると、図1に示すICカード104の詳細な構成例が示されている。

【0073】ICカードは制御部401、入出力部402、復号部403、暗号部404、圧縮部405、乱数発生部406、認証部407、ICカード秘密鍵記憶部408、管理センタ公開鍵記憶部409、ICカード公開鍵証明書記憶部410、再生装置公開鍵証明書記憶部411、コンテンツ暗号鍵記憶部412、タイマ413、電池414から構成される。

【0074】ICカード秘密鍵記憶部408には、ICカードの秘密鍵が記憶されている。

【0075】管理センタ公開鍵記憶部409は、管理センタの公開鍵が記憶されている。

【0076】ICカード公開鍵証明書記憶部410は、管理センタ101が発行したICカード公開鍵証明書が記憶される。

【0077】再生装置公開鍵証明書記憶部411には、管理センタ101が発行した再生装置公開鍵証明書であって再生装置106から読み出されたものが記憶される。

【0078】コンテンツ暗号鍵記憶部412は電池414でバックアップされており、管理センタ101から配布を受ける暗号化されたコンテンツ暗号鍵をタイマ413が所定の値に変化するまで記憶する。

【0079】タイマ413は電池414でバックアップされており、管理センタ101から配布されたタイマの初期値から時間と共に変化し所定の値になるとコンテンツ暗号鍵記憶部412に記憶されているコンテンツ暗号鍵を消去する。

【0080】復号部403は入出力部402を介して店舗の端末103あるいはユーザが所有する再生装置106からの暗号化データを受信すると制御部401の制御

により、ICカード秘密鍵、あるいは管理センタ公開鍵を使って暗号化データを復号する。

【0081】暗号部404は、入出力部402を介して店舗の端末103あるいはユーザが所有する再生装置106へデータを送信する時、制御部101の制御によりICカード秘密鍵あるいは再生装置の公開鍵を使いデータを暗号化する。

【0082】圧縮部405はハッシュ関数を用いて制御部401の制御により任意のデータの圧縮を行う。

【0083】乱数発生部406は制御部401の制御により乱数を発生する。

【0084】認証部407は相互認証時に送信した乱数と受信した乱数の照合と、受信したデータと署名データの照合を行う。

【0085】図5を参照すると、図1に示す再生装置106の詳細な構成例が示されている。

【0086】再生装置106は制御部501と、ICカード入出力部502と、復号部503と、暗号部504と、圧縮部505と、乱数発生部506と、認証部507と、操作入力部508と、コンテンツ記録媒体入出力部509と、再生装置秘密鍵記憶部510と、管理センタ公開鍵記憶部511と、再生装置公開鍵証明書記憶部512と、タイマ513と、コンテンツ暗号鍵記憶部514と、コンテンツ暗号鍵復号部515と、コンテンツ再生部516とで構成されている。

【0087】再生装置秘密鍵記憶部510には、再生装置106の秘密鍵が記憶されている。

【0088】管理センタ公開鍵記憶部511は、管理センタ公開鍵が記憶されている。

【0089】再生装置公開鍵証明書記憶部512には管理センタ101が発行した再生装置公開鍵証明書が記憶されている。

【0090】タイマ513には、ICカード入出力部502を介してICカード104から読み出されたレンタル期間を示す所定のタイマ値が制御部501により書き込まれる。タイマ513のタイマ値は時間と共に変化し、タイマ513は、タイマ513のタイマ値がレンタル期間が終了する所定の値になるとコンテンツ暗号鍵記憶部514に記憶されているコンテンツ暗号鍵をクリアする。

【0091】コンテンツ暗号鍵記憶部514には、制御部501がICカード入出力部502を介してICカード104から読み出した暗号化されたコンテンツ暗号鍵が記憶される。

【0092】復号部503はICカード入出力部502を介してICカード104から暗号化データやデジタル署名データを受信すると制御部501の制御により、再生装置秘密鍵、あるいは管理センタ公開鍵を使って暗号化データやデジタル署名データを復号する。

【0093】暗号部504はICカード入出力部502

を介してICカード104へデータを送信する時、制御部101の制御により再生装置秘密鍵を使いデータを暗号化する。

【0094】圧縮部505はハッシュ関数を用いて制御部501の制御により任意のデータの圧縮を行う。

【0095】乱数発生部506は制御部501の制御により乱数を発生する。

【0096】認証部507は相互認証時に送信した乱数と受信した乱数の照合と、受信したデータと署名データの照合を行う。

【0097】次に図1の再生装置106とICカード104の相互認証の動作を図6に示すタイムチャートを用いて順に説明する。

【0098】この相互認証はICカード104と再生装置106の工場出荷前、ユーザが本システムを初めて利用する時、再生装置106の機種変更時、及びコンテンツ再生時に行われる。

【0099】まず、再生装置106へICカード104を接続する(S101)。

【0100】再生装置106の制御部501はICカード入出力部502を介してICカード104の接続を確認し、認識されるまで処理を繰り返す(S102)。

【0101】再生装置106の制御部501はICカード入出力部502を介してICカード104の接続を確認すると、ICカード104に対して再生装置公開鍵証明書記憶部512に記憶されている再生装置公開鍵証明書(PK_{pl}, S1)と共に相互認証の要求をICカード入出力部502を介して行う(S103)。

【0102】次に、ICカード104の制御部401は入出力部402を介して再生装置公開鍵証明書PK_{pl}, S1と共に相互認証の要求を受信すると、管理センタ公開鍵記憶部409に記憶されている管理センタ公開鍵PK_{cnt}を用いて再生装置公開鍵証明書の署名S1を復号部403にて復号しPK_{cnt}(S1)を生成し、圧縮部405にてハッシュ関数を用いて再生装置公開鍵PK_{pl}を圧縮しH(PK_{pl})を生成し、認証部407にてPK_{cnt}(S1)とH(PK_{pl})を照合する(S104)。

【0103】S105においてPK_{cnt}(S1)とH(PK_{pl})が不一致である場合、ICカード104の制御部401は再生装置106から受信した再生装置公開鍵証明書を管理センタ101が発行していない不正な再生装置公開鍵証明書であると判断し、入出力部402を介して再生装置106へエラー通知を行う(S106)。

【0104】再生装置106の制御部501はICカード入出力部502を介してエラー通知を受信すると(S107)、相互認証を中止する(S130)。

【0105】S105においてPK_{cnt}(S1)とH(PK_{pl})が一致した場合、ICカード104の制御

部401は再生装置106から受信した再生装置公開鍵証明書を管理センタ101が発行した正当な再生装置公開鍵証明書である判断し、ICカード公開鍵証明書記憶部410に記憶されているICカード公開鍵証明書(PK_{ic}, S2)を再生装置106へ入出力部402を介して送信する(S108)。

【0106】再生装置106の制御部501はICカード入出力部502を介してICカード公開鍵証明書(PK_{ic}, S2)を受信すると、管理センタ公開鍵記憶部511に記憶している管理センタ公開鍵PK_{cnt}を用いて署名S2を復号部503にて復号しPK_{cnt}(S2)を生成し、圧縮部505にてハッシュ関数を用いてICカード公開鍵PK_{ic}を圧縮しH(PK_{ic})を生成し、認証部507にてPK_{cnt}(S2)とH(PK_{ic})を照合する(S109)。

【0107】S110において、PK_{cnt}(S2)とH(PK_{ic})が不一致である場合、再生装置106の制御部501は、ICカード104から受信したICカード公開鍵証明書が管理センタ101が発行していない不正なICカード公開鍵証明書であると判断し相互認証を中止する(S130)。

【0108】S110において、PK_{cnt}(S2)とH(PK_{ic})が一致した場合、再生装置106の制御部501は、ICカード104から受信したICカード公開鍵証明書を管理センタ101が発行した正当なICカード公開鍵証明書であると判断し、次に乱数発生部506で乱数R_{pl}を生成する(S111)。

【0109】再生装置106の制御部501はICカード公開鍵PK_{ic}を用いて乱数R_{pl}を暗号部504にて暗号化しPK_{ic}(R_{pl})を生成し(S112)、PK_{ic}(R_{pl})をICカード104へICカード入出力部502を介して送信する(S113)。

【0110】ICカード104の制御部401は入出力部402を介してPK_{ic}(R_{pl})を受信すると、ICカード秘密鍵記憶部408に記憶しているICカード秘密鍵SK_{ic}を用いてPK_{ic}(R_{pl})を復号部403にて復号しDR_{pl}を生成する(S114)。

【0111】次に乱数発生部406で乱数R_{ic}を生成し(S115)、再生装置公開鍵PK_{pl}を用いて乱数R_{ic}を暗号部404にて暗号化しPK_{pl}(R_{ic})を生成し(S116)、PK_{pl}(R_{ic})とDR_{pl}を入出力部402を介して再生装置106へ送信する(S117)。

【0112】再生装置106の制御部501はICカード入出力部502からPK_{pl}(R_{ic})とDR_{pl}を受信すると(S118)、再生装置106がステップS111で生成した乱数R_{pl}とICカード104がステップS114で復号したDR_{pl}を認証部507で照合する(S119)。

【0113】S119において、R_{pl}とDR_{pl}が不

一致である場合、再生装置106の制御部501は、ICカード104がICカード104から受信してあるICカード公開鍵とペアではないICカード秘密鍵を保持した不正なICカードである判断し相互認証を中止する(S130)。

【0114】S119において、RplとDRplが一致した場合、再生装置106の制御部501は、ICカード104がICカード104から受信してあるICカード公開鍵とペアであるICカード秘密鍵を保持した正当なICカードであると判断し、再生装置秘密鍵記憶部510に記憶されている再生装置秘密鍵SKplを用いてS118にて受信したPKpl(Ric)を復号部503で復号しDRicを生成し(S120)、ICカード入出力部502を介してICカード104へDRicを送信する(S121)。

【0115】ICカード104の制御部401は入出力部402からDRicを受信すると(S122)、ICカード104がステップS115で生成した乱数Ricと再生装置106がステップS120で復号したDRicを認証部407で照合する(S123)。

【0116】S123において、RicとDRicが不一致である場合、ICカード104の制御部401は入出力部402を介して再生装置106へエラー通知を行う(S124)。

【0117】再生装置106の制御部501はICカード入出力部502からエラー通知を受信すると(S125)、相互認証を中止する(S130)。

【0118】S123において、RicとDRicが一致した場合、ICカード104の制御部401は再生装置公開鍵証明書記憶部411の内容と、S104で受信した再生装置公開鍵証明書(PKpl, S)を比較する(S126)。

【0119】S126において、再生装置公開鍵証明書記憶部411の内容と、S104で受信した再生装置公開鍵証明書(PKpl, S)が異なる場合、S104で受信した再生装置106の公開鍵証明書(PKpl, S)を再生装置公開鍵証明書記憶部411に記憶する(S127)。

【0120】S126において、再生装置公開鍵証明書記憶部411の内容と、S104で受信した再生装置公開鍵証明書(PKpl, S)が等しい場合、S128へ遷移する。

【0121】次にICカード104の制御部401は相互認証の正常終了を入出力部402を介して再生装置106へ通知し(S128)、再生装置106の制御部501はICカード入出力部502を介して相互認証の正常終了を受信すると相互認証を終了する(S129)。

【0122】次に図1に示すICカード104と管理センタ101の相互認証の動作を図7に示すタイムチャートを使用して説明する。

【0123】ユーザはICカード104とコンテンツ記録媒体105を店舗の端末103へ持参しICカード104とコンテンツ記録媒体105を端末103へ接続する(S201)。

【0124】端末103の制御部301はICカード入出力部303を介してICカード104の接続を確認すると(S202)、ICカード104の相互認証を実施するため、制御部301はICカード公開鍵証明書の読み出し要求をICカード入出力部303を介してICカード104へ通知する(S203)。

【0125】ICカード104の制御部401は入出力部402からICカード104の公開鍵証明書の読み出し要求を受信すると、ICカード公開鍵証明書記憶部410に記憶されているICカード公開鍵証明書(PKic, S2)を入出力部402を介して端末103へ送信する(S204)。

【0126】次に、端末103の制御部301はICカード入出力部303からICカード公開鍵証明書(PKic, S2)を受信すると、通信部302からネットワーク102を介して管理センタ101へICカード公開鍵証明書(PKic, S2)と共に相互認証を要求する(S205)。

【0127】管理センタ101の制御部201は通信部207を介して端末103からの相互認証要求とICカード公開鍵証明書(PKic, S2)を受信すると(S206)、公開鍵データベース211からICカード公開鍵証明書(PKic, S2)中のICカード公開鍵PKicと同一のICカード公開鍵を検索しICカード公開鍵PKicが有効であるか確認する(S207)。

【0128】S207において、ICカード公開鍵PKicが不正あるいは失効している場合、管理センタ101の制御部201は相互認証要求の応答として通信部207からネットワーク102を介して端末103へエラー通知を送信し(S208)、端末103の制御部301は通信部302を介してS208のエラー通知を受信すると相互認証処理を中止する(S230)。

【0129】S207によりICカード公開鍵PKicが有効であると判断した場合、S206で受信したICカード公開鍵証明書(PKic, S2)の署名S2を管理センタ公開鍵記憶部209に記憶されている管理センタ公開鍵PKcntを用いて復号部203にて復号しPKcnt(S2)を生成し、PKicを圧縮部204にてハッシュ関数を用いて圧縮しH(PKic)を生成し、次に認証部206にてPKcnt(S2)とH(PKic)が等しいか照合する(S208)。

【0130】S209において、PKcnt(S2)とH(PKic)が不一致の場合、管理センタ101の制御部201は、ステップS206で受信した公開鍵証明書(PKic, S2)が管理センタ101が発行していない公開鍵証明書であると判断して通信部207からネ

ットワーク102を介して端末103へエラーを通知し(S210)、端末103の制御部301はS210より通信部302を介してエラー通知を受信すると相互認証を中止する(S230)。

【0131】S209において、PKcnt (S2)とH (PKic) が一致した場合、管理センタ101の制御部201は、S206で受信したICカード公開鍵証明書(PKic, S2)が管理センタ101が発行した公開鍵証明書であると判断して乱数発生部205で乱数Rcntを発生させ(S211)、ICカード公開鍵PKicを用いて暗号部203にて乱数Rcntを暗号化しPKic (Rcnt)を生成し(S212)、通信部207からネットワーク102を介して端末103へ相互認証要求の応答データとしてPKic (Rcnt)を送信する(S213)。

【0132】端末103の制御部301は、通信部302から暗号データPKic (Rcnt)を受信すると、ICカード入出力部303を介してICカード104へPKic (Rcnt)を送信する(S214)。

【0133】ICカード104の制御部401は、入出力部402からはPKic (Rcnt)を受信すると、復号部403にてICカード秘密鍵記憶部408に記憶されているICカード秘密鍵SKicを用いてPKic (Rcnt)を復号部403で復号しDRcntを生成する(S215)。

【0134】次にICカード104の制御部401は乱数発生部406にて乱数Ricを発生し(S216)、暗号部404にて管理センタ公開鍵PKcntを用いて暗号部404で暗号化しPKcnt (Ric)を生成し(S217)、相互認証要求の応答データとしてPKcnt (Ric)とDRcntを入出力部402から端末103へ送信する(S218)。

【0135】端末103の制御部301はICカード入出力部303からPKcnt (Ric)とDRcntを受信すると、管理センタ101へ相互認証要求の応答データとして通信部302からネットワーク102を介してPKcnt (Ric)とDRcntを送信する(S219)。

【0136】管理センタ101の制御部201は通信部207からPKcnt (Ric)とDRcntを受信すると(S220)、認証部206にて復号データDRcntとステップ211で発生した乱数データRcntを照合する(S221)。

【0137】S221において、DRcntとRcntが不一致である場合、管理センタ101の制御部201は、ICカード104がICカード公開鍵PKicのペアであるICカード秘密鍵を保持していない不正なICカードと判断し、通信部207からネットワーク102を介して端末103へエラー通知し(S222)、端末

103の制御部301は通信部302からエラー通知を受信すると相互認証を中止する(S230)。

【0138】S221において、DRcntとRcntが一致する場合、管理センタ101の制御部201は、ICカード104がICカード公開鍵PKicのペアであるICカード秘密鍵を保持している正当なICカードであると判断し、復号部202にて管理センタ秘密鍵記憶部208に記憶している管理センタ秘密鍵SKcntを用いてPKcnt (Ric)を復号しDRicを生成し通信部207からネットワーク102を介して端末103へDRicを送信する(S223)。

【0139】端末103の制御部301は通信部302からDRicを受信すると、ICカード入出力部303を介してICカード104へDRicを送信する(S224)。

【0140】次にICカード104の制御部401は入出力部402を介して端末103からDRicを受信すると(S225)、ステップS216で発生した乱数RicとDRicを認証部407にて照合する(S226)。

【0141】S226において、乱数RicとDRicが不一致である場合、ICカード104の制御部401は、管理センタ101が管理センタ秘密鍵SKcntを保持していない不正な相手と判断し、入出力部402から端末103へエラー通知し(S227)、端末103の制御部301はICカード入出力部303からエラー通知を受信すると相互認証を中止する。

【0142】S226において、Ricと復号データDRicが一致した場合、ICカード104の制御部401は、管理センタ101が管理センタ秘密鍵SKcntを保持している正当な管理センタであると判断し、入出力部402から端末103へ正常終了の通知を送信し(S228)、端末103の制御部301はICカード入出力部303から正常終了の通知を受信すると相互認証を正常終了する(S229)。

【0143】図8は、上記のICカード104と管理センタ101の相互認証終了後のICカード104から管理センタ101への再生装置公開鍵証明書の転送処理を示している。

【0144】まず端末103の制御部301はICカード入出力部303からICカード104へ再生装置公開鍵証明書の読み出し要求する(S301)。

【0145】ICカード104の制御部401は入出力部402を介して端末103から再生装置公開鍵証明書の読み出し要求を受信すると、再生装置公開鍵証明書記憶部411に記憶している再生装置公開鍵証明書(PKpl, S1)を入出力部402から端末103へ送信する(S302)。

【0146】端末103の制御部301はICカード入出力部303から再生装置公開鍵証明書(PKpl, S

1)を受信すると、通信部302からネットワーク102を介して管理センタ101へ再生装置公開鍵証明書(PKpl, S1)を送信する(S304)。

【0147】管理センタ101の制御部201は通信部207を介して端末103から再生装置公開鍵証明書(PKpl, S1)を受信すると(S305)、再生装置公開鍵証明書(PKpl, S1)中の公開鍵PKplと同一の公開鍵を公開鍵データベース211から検索し、その公開鍵が有効な公開鍵であるか検証する(S306)。

【0148】S306において、S305で受信した再生装置公開鍵証明書が不正あるいは失効している場合、管理センタ101の制御部201は通信部207からネットワークを介して端末103へエラー通知をし(S307)、端末103の制御部301は通信部302からエラー通知を受信すると再生装置公開鍵証明書の転送処理を中止する(S313)。

【0149】S306において、S305で受信した再生装置公開鍵証明書が正当であると判断した場合、管理センタ公開鍵記憶部209に記憶している管理センタ公開鍵PKcntを用いて再生装置公開鍵証明書(PKpl, S1)中の署名S1を復号部202で復号しPKcnt(S1)を生成し、ハッシュ関数を用いて再生装置公開鍵証明書(PKpl, S1)中のPKplを圧縮部204で圧縮しH(PKpl)を生成し、PKcnt(S1)とH(PKpl)を認証部206にて照合する(S308)。

【0150】S309において、PKcnt(S1)とH(PKpl)が不一致である場合、管理センタ101の制御部201は、再生装置106が再生装置公開鍵PKplとペアである再生装置秘密鍵SKplを保持しない不正な再生装置であると判断し、通信部207からネットワーク102を介して端末103へエラー通知を送信し(S310)、端末103の制御部301は通信部302からエラー通知を受信すると再生装置公開鍵証明書の転送処理を中止する(S313)。

【0151】S309において、PKcnt(S1)とH(PKpl)が一致した場合、管理センタ101の制御部201は、再生装置106が再生装置公開鍵PKplとペアである再生装置秘密鍵SKplを保持した正当な再生装置であると判断し、通信部202からネットワーク102を介して端末103へ正常終了通知し(S311)、端末103の制御部301は通信部302から正常終了の通知を受信すると再生装置公開鍵証明書の転送処理を正常終了する(S312)。

【0152】図9は、上記の再生装置公開鍵証明書の転送処理の後に行われるコンテンツの再生に必要な情報のダウンロード処理のタイムチャートを示している。

【0153】まず、ユーザは端末103の表示部306からレンタルするコンテンツを選択し、入力部305に

てコンテンツのタイトルCとレンタル期間Tを入力する(S401)。

【0154】コンテンツのタイトルCとレンタル期間Tを含む契約内容を契約情報CTとして、端末103の制御部301は契約情報CTと共に契約データ作成要求をICカード入出力部303を介してICカード104へ送信する(S402)。

【0155】ICカード104の制御部401は入出力部402から契約データ作成要求と契約情報CTを受信すると、契約情報CTを圧縮部405にてハッシュ関数を用いて圧縮しH(CT)を生成し、ICカード秘密鍵記憶部408に記憶しているICカード秘密鍵SKicを用いてH(CT)を暗号部404で暗号化することにより契約情報へのICカード秘密鍵による署名S3を生成する(S403)。

【0156】次にICカード104の制御部401は、入出力部402を介して契約情報CTと署名S3を端末103へ送信する(S404)。

【0157】端末103の制御部301はICカード入出力部303から契約情報CTと署名S3を受信すると、通信部302からネットワーク102を介して管理センタ101へ契約情報CTと署名S3と共にコンテンツ暗号鍵のダウンロード要求を送信する(S405)。

【0158】管理センタ101の制御部201は通信部207からコンテンツ暗号鍵ダウンロード要求と契約情報CTと署名S3を受信すると(S406)、上記の相互認証によって正常と確認されたICカードの公開鍵PKicを用いてS3を復号部202で復号しPKic(S3)を生成し、圧縮部204にてハッシュ関数を用いて契約情報CTを圧縮しH(CT)を生成し、認証部206にてPKic(S3)とH(CT)を照合する(S407)。

【0159】S408において、PKic(S3)とH(CT)が不一致である場合、管理センタ101の制御部201は、ICカード104が不正あるいは契約情報CT及び/又は署名S3が改竄されたと判断し通信部207からネットワーク102を介して端末103へエラー通知し(S409)、端末103の制御部301は通信部302からエラー通知を受信するとコンテンツ暗号鍵ダウンロード処理を中止する(S426)。

【0160】S408において、PKic(S3)とH(CT)が一致した場合、管理センタ101の制御部201は、契約情報CTの発行者がICカード104である特定しかつ契約情報CT及び/又は署名S3に改竄が加えられていないと判断し、課金データベース212を契約情報CTにより更新する(S410)。

【0161】次に管理センタ101の制御部201は、契約情報CTに含まれるコンテンツのタイトルに対応したコンテンツ暗号鍵CKをコンテンツ暗号鍵記憶部209から読み出し、コンテンツ暗号鍵CKを圧縮部204

にてハッシュ関数を用いて圧縮しH (CK) を生成し、管理センタ秘密鍵記憶部208に記憶している管理センタ秘密鍵SKcntを用いてH (CK) を暗号部203で暗号化することによりコンテンツ暗号鍵への管理センタ秘密鍵による署名S4を生成する(S411)。

【0162】次に上記の再生装置公開鍵の転送処理によって正常と確認された再生装置公開鍵PKplを用いて、暗号部203にてコンテンツ暗号鍵CKと署名S4を暗号化しPKpl (CK, S4) を生成する(S412)。

【0163】次に圧縮部204にてハッシュ関数を用いてPKpl (CK, S4) と契約情報CTを圧縮しH (PKpl (CK, S4), CT) を生成し、暗号部203にて管理センタ秘密鍵SKcntを用いて、H (PKpl (CK, S4), CT) を暗号化し署名S5を生成する(S413)。

【0164】次に暗号部203にてICカード公開鍵PKicを用いて、暗号化されたコンテンツ暗号鍵PKpl (CK, S4) と契約情報CTと署名S5を暗号化しPKic (PKpl (CK, S4), CT, S5) を生成する(S414)。

【0165】次にコンテンツ暗号鍵ダウンロード要求に対するコンテンツ暗号鍵データとしてPKic (PKpl (CK, S4), CT, S5) を通信部207からネットワーク102を介して端末103へ送信する(S415)。

【0166】端末103の制御部301は通信部302からコンテンツ暗号鍵データPKic (PKpl (CK, S4), CT, S5) を受信すると、ICカード入出力部303を介してICカード104へコンテンツ暗号鍵データPKic (PKpl (CK, S4), CT, S5) と共にコンテンツ暗号鍵記憶要求を送信する(S416)。

【0167】ICカード104の制御部401は入出力部402からコンテンツ暗号鍵記憶要求とコンテンツ暗号鍵データPKic (PKpl (CK, S4), CT, S5) を受信すると、復号部403にてICカード秘密鍵記憶部408に記憶しているICカード秘密鍵SKicを用いてPKic (PKpl (CK, S4), CT, S5) を復号しPKpl (CK, S4) と契約情報CTと署名S5を生成する(S417)。

【0168】次に復号部403にて管理センタ公開鍵記憶部409に記憶している管理センタ公開鍵PKcntを用いて署名S5を復号しPKcnt (S5) を生成し、圧縮部405にてハッシュ関数を用いてPKpl (CK, S4) と契約情報CTを圧縮しH (PKpl (CK, S4), CT) を生成し、認証部407にてPKcnt (S5) とH (PKpl (CK, S4), CT) を照合する(S418)。

【0169】S419において、PKcnt (S5) と

H (PKpl (CK, S4), CT) が不一致である場合、ICカード104の制御部401は、受信したデータは管理センタ101に成りすました装置からの不正なデータであるかあるいは改竄を加えられたデータであると判断し入出力部402を介して端末103へエラー通知を送信し(S420)、端末103の制御部301はICカード入出力部303からエラー通知を受信するとコンテンツ暗号鍵ダウンロード処理を中止する(S426)。

【0170】S419において、PKcnt (S5) とH (PKpl (CK, S4), CT) が一致した場合、ICカード104の制御部401は、受信したデータの発行者は管理センタ101であると特定し、かつ受信したデータは改竄されていないと判断し、契約情報CT中の契約期限データTをタイマ413へセットし(S421)、暗号化コンテンツ暗号鍵PKpl (CK, S4) をコンテンツ暗号鍵記憶部412へセットする(S422)。

【0171】次にICカード104の制御部401は入出力部402を介して端末103へコンテンツ暗号鍵記憶要求に対するの正常応答を送信し(S423)、端末103の制御部301はICカード入出力部303から正常終了を受信するとコンテンツ記憶部307からコンテンツデータをコンテンツ記憶媒体105へ書き込む(S424)。

【0172】コンテンツ記録媒体105へのコンテンツデータの書き込みが終了するとユーザはICカード104とコンテンツ記録媒体105を持ち帰る(S425)。

【0173】図10は図1の再生装置106とICカード104とコンテンツ記憶媒体105を利用してコンテンツを再生する処理のタイムチャートを示している。

【0174】まずユーザは再生装置106へICカード104を接続し、再生装置106とICカード104は相互認証を行う(S501)。ICカード104と再生装置103の相互認証は既に説明したので、ここでは省略する。

【0175】再生装置106の制御部501は操作入力部508からのコンテンツの再生指示(S502)により、ICカード入出力部502を介してICカード104へコンテンツ暗号鍵の送信を要求する(S503)。

【0176】ICカード104の制御部401は入出力部402からコンテンツ暗号鍵の送信要求を受信すると(S504)、コンテンツ暗号鍵記憶部412にコンテンツ暗号鍵が存在しているか確認する(S505)。

【0177】S505において、コンテンツ暗号鍵記憶部412にコンテンツ暗号鍵が無い場合、ICカード104の制御部401は入出力部402を介して再生装置106へコンテンツ暗号鍵の消去通知を送信し(S506)、再生装置106の制御部501はコンテンツ暗号

鍵の消去通知を受信するとコンテンツ再生不可としてコンテンツ再生処理を終了する (S520)。

【0178】S505において、コンテンツ暗号記憶部412にコンテンツ暗号鍵がある場合、ICカード104の制御部401は、コンテンツ暗号鍵記憶部412から暗号化されたコンテンツ暗号鍵PKpl (CK, S4)を、タイマ413からタイマ値tを読み出し (S508)、圧縮部405にてハッシュ関数を用いてコンテンツ暗号鍵PKpl (CK, S4)とタイマ値tを圧縮しH (PKpl (CK, S4), t)を生成し、暗号部404にてICカード秘密鍵記憶部408に記憶されているICカード秘密鍵SKicを用いてH (PKpl (CK, S4), t)を暗号化することにより署名S6を生成する (S509)。

【0179】次にICカード104の制御部401は再生装置公開鍵により暗号化されているコンテンツ暗号鍵PKpl (CK, S4)とタイマ値tと署名S6を入出力部402を介して再生装置106へ送信する (S510)。

【0180】再生装置106の制御部501はICカード入出力部502から再生装置公開鍵により暗号化されているコンテンツ暗号鍵PKpl (CK, S4)とタイマ値tと署名S6を受信すると、復号部503にて上記の相互認証で正常と確認されたICカード公開鍵PKicを用いて署名S6を復号しPKic (S6)を生成し、圧縮部505にてハッシュ関数を用いてコンテンツ暗号鍵PKpl (CK, S4)とタイマ値tを圧縮しH (PKpl (CK, S4), t)を生成し、認証部507にてPKic (S6)とH (PKpl (CK, S4), t)を照合する (S511)。

【0181】S512において、PKic (S6)とH (PKpl (CK, S4), t)が不一致である場合、再生装置106の制御部501は、受信したデータは正当なICカードになりすましたICカードからのデータであるか又はICカード104から受信したデータは改竄されていると判断し、再生不可として再生処理を終了する (S520)。

【0182】S512において、PKic (S6)とH (PKpl (CK, S4), t)が一致した場合、再生装置106の制御部501はタイマ値tをタイマ513へセット (S513)する。

【0183】次に再生装置106の制御部501は復号部503にて再生装置秘密鍵記憶部510に記憶されている再生装置秘密鍵SKplを用いて再生装置公開鍵により暗号化されているコンテンツ暗号鍵PKpl (CK, S4)を復号しCKと署名S4を生成する (S514)。

【0184】次に復号部503にて管理センタ公開鍵記憶部511に記憶されている管理センタ公開鍵PKcntを用いて署名S4を復号しPKcnt (S4)を生成

し、圧縮部505にてハッシュ関数を用いてCKを圧縮しH (CK)を生成し、認証部507でPKcnt (S4)とH (CK)を照合する (S515)。

【0185】S516において、PKcnt (S4)とH (CK)が不一致である場合、再生装置106の制御部501は、受信したデータが管理センタ101が発行したデータではないかあるいはデータが改竄されていると判断し再生不可として再生処理を終了する (S520)。

【0186】S516において、PKcnt (S4)とH (CK)が一致した場合、再生装置106の制御部501はコンテンツ暗号鍵CKをコンテンツ暗号鍵記憶部514へセットする (S517)。

【0187】次に、再生装置106の制御部501はコンテンツ記録媒体入出力部509を介してコンテンツ記録媒体105からコンテンツデータを読み出し、コンテンツ再生部516にてコンテンツ暗号鍵記憶部515に記憶されているコンテンツ暗号鍵CKを用いてコンテンツデータを復号し (S518)、コンテンツ再生を行う (S519)。

【0188】

【発明の効果】以上説明したように本発明によれば、以下の効果が奏される。

【0189】第1に、再生装置の公開鍵証明書はICカードへ記憶することで再生をすることが可能な再生装置を安全に限定することかできる。

【0190】第2に、コンテンツをレンタルする前に再生装置の公開鍵証明書をICカードへ記憶することで、再生装置の機種を安全かつ柔軟に変更することが可能であり、変更後の再生装置のみを再生をすることができる再生装置として安全に限定できる。

【0191】第3に、有効なコンテンツ暗号鍵、再生期限情報及び公開鍵証明書は管理センタが発行したものに限定されるので、有効なコンテンツ暗号鍵、再生期限情報及び公開鍵証明書は一元管理の基に保証され、従って、安全なコンテンツの流通が可能になる。

【0192】第4に、ICカードの内部に再生期限情報を記憶しリアルタイムに再生期限を減ずる機能を有することで、再生期限の改竄を防止できる。

【0193】第5に、ICカードならびに再生装置の内部に再生期限を過ぎるとコンテンツ再生に必要なコンテンツ暗号鍵を消去する機能を有することで、耐タンパ性を向上できる。

【図面の簡単な説明】

【図1】本発明の実施の形態におけるレンタルコンテンツ流通システムを示すブロック図である。

【図2】本発明の実施の形態における管理センタを示すブロック図である。

【図3】本発明の実施の形態における端末を示すブロック図である。

【図４】本発明の実施の形態におけるＩＣカードを示すブロック図である。

【図５】本発明の実施の形態における再生装置を示すブロック図である。

【図６】本発明の実施の形態におけるＩＣカードと再生装置の相互認証を示すタイムチャートである。

【図７】本発明の実施の形態におけるＩＣカードと管理センタの相互認証を示すタイムチャートである。

【図８】本発明の実施の形態におけるＩＣカードから管理センタへ再生装置公開鍵証明書の転送を示すタイムチャートである。

【図９】本発明の実施の形態における管理センタからＩＣカードへのコンテンツ暗号鍵のダウンロードを示すタイムチャートである。

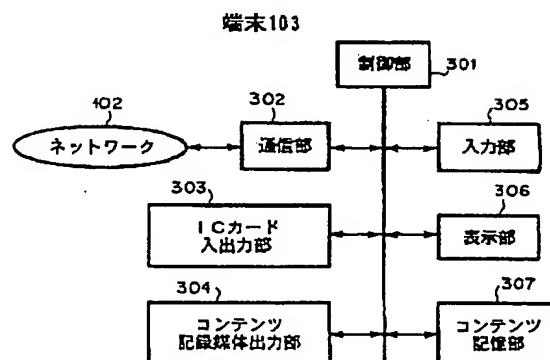
【図１０】本発明の実施の形態におけるコンテンツ再生を示すタイムチャートである。

【符号の説明】

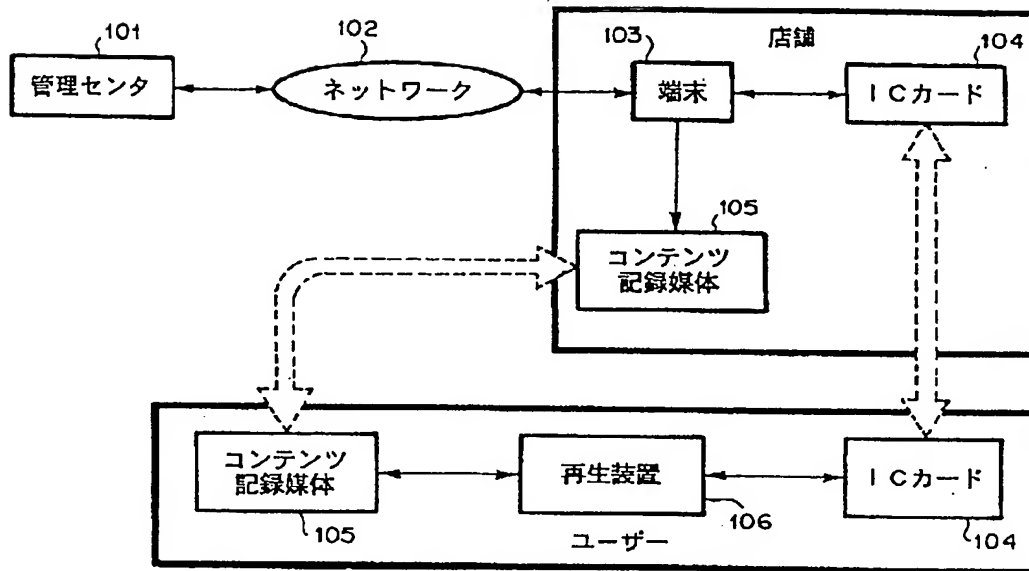
101 管理センタ
102 ネットワーク
103 端末
104 ＩＣカード
105 コンテンツ記録媒体
106 再生装置
201 制御部
202 復号部
203 暗号部
204 圧縮部
205 乱数発生部
206 認証部
207 通信部
208 管理センタ秘密鍵記憶部
209 管理センタ公開鍵記憶部
210 コンテンツ暗号鍵記憶部
211 公開鍵データベース
212 課金情報データベース
301 制御部
302 通信部
303 ＩＣカード入出力部
304 コンテンツ記録媒体出力部
305 入力部
306 表示部
307 コンテンツ記憶部

302 通信部
303 ＩＣカード入出力部
304 コンテンツ記録媒体入出力部
305 入力部
306 表示部
307 コンテンツ記憶部
401 制御部
402 入出力部
403 復号部
404 暗号部
405 圧縮部
406 乱数発生部
407 認証部
408 ＩＣカード秘密鍵記憶部
409 管理センタ公開鍵記憶部
410 ＩＣカード公開鍵証明書記憶部
411 再生装置公開鍵証明書記憶部
412 コンテンツ暗号鍵記憶部
413 タイマ
414 電池
501 制御部
502 ＩＣカード入出力部
503 復号部
504 暗号部
505 圧縮部
506 乱数発生部
507 認証部
508 操作入力部
509 コンテンツ記録媒体入出力部
510 再生装置秘密鍵記憶部
511 管理センタ公開鍵記憶部
512 再生装置公開鍵証明書
513 タイマ
514 コンテンツ暗号鍵記憶部
515 コンテンツ暗号鍵復号部
516 コンテンツ再生部

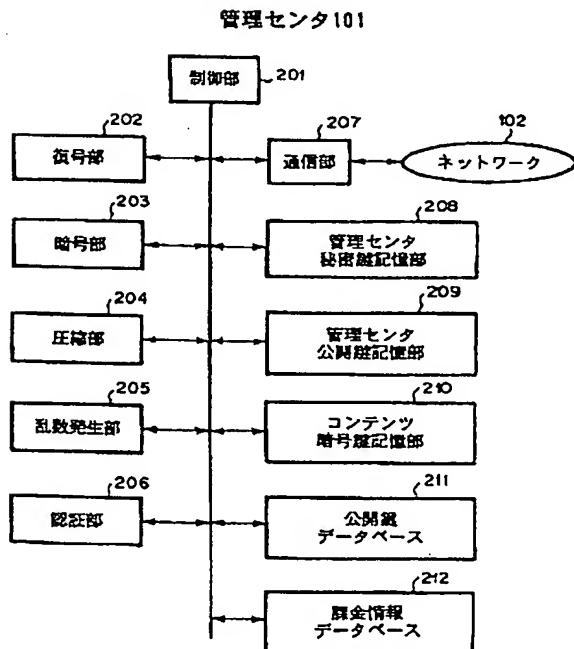
【図３】



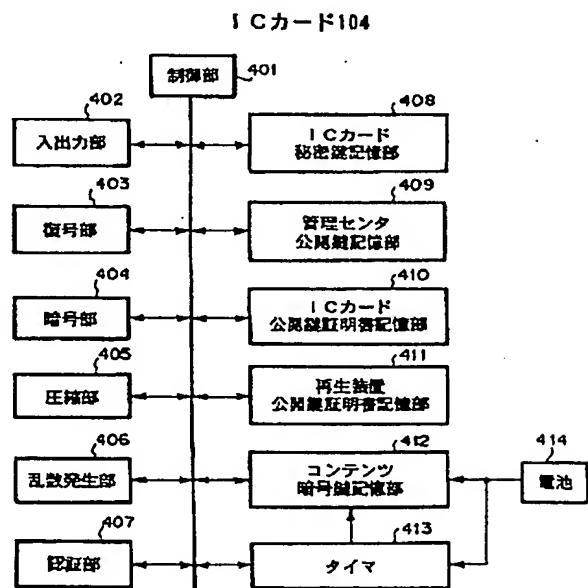
【図 1】



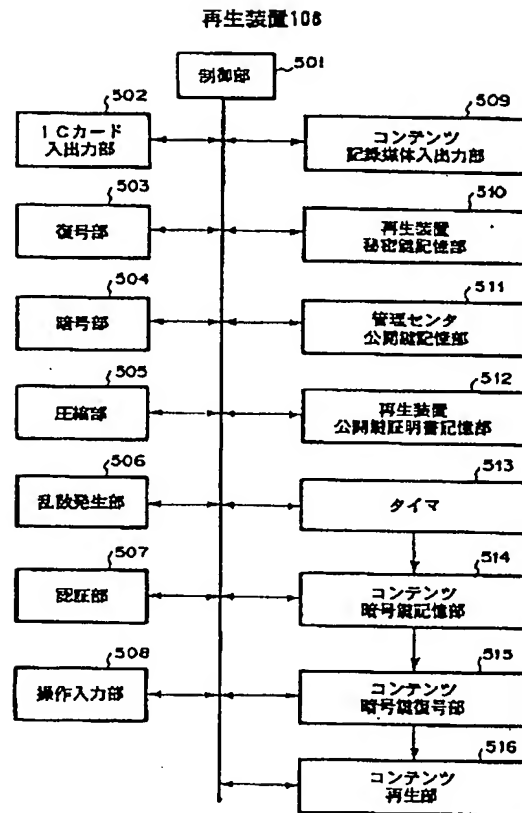
【図 2】



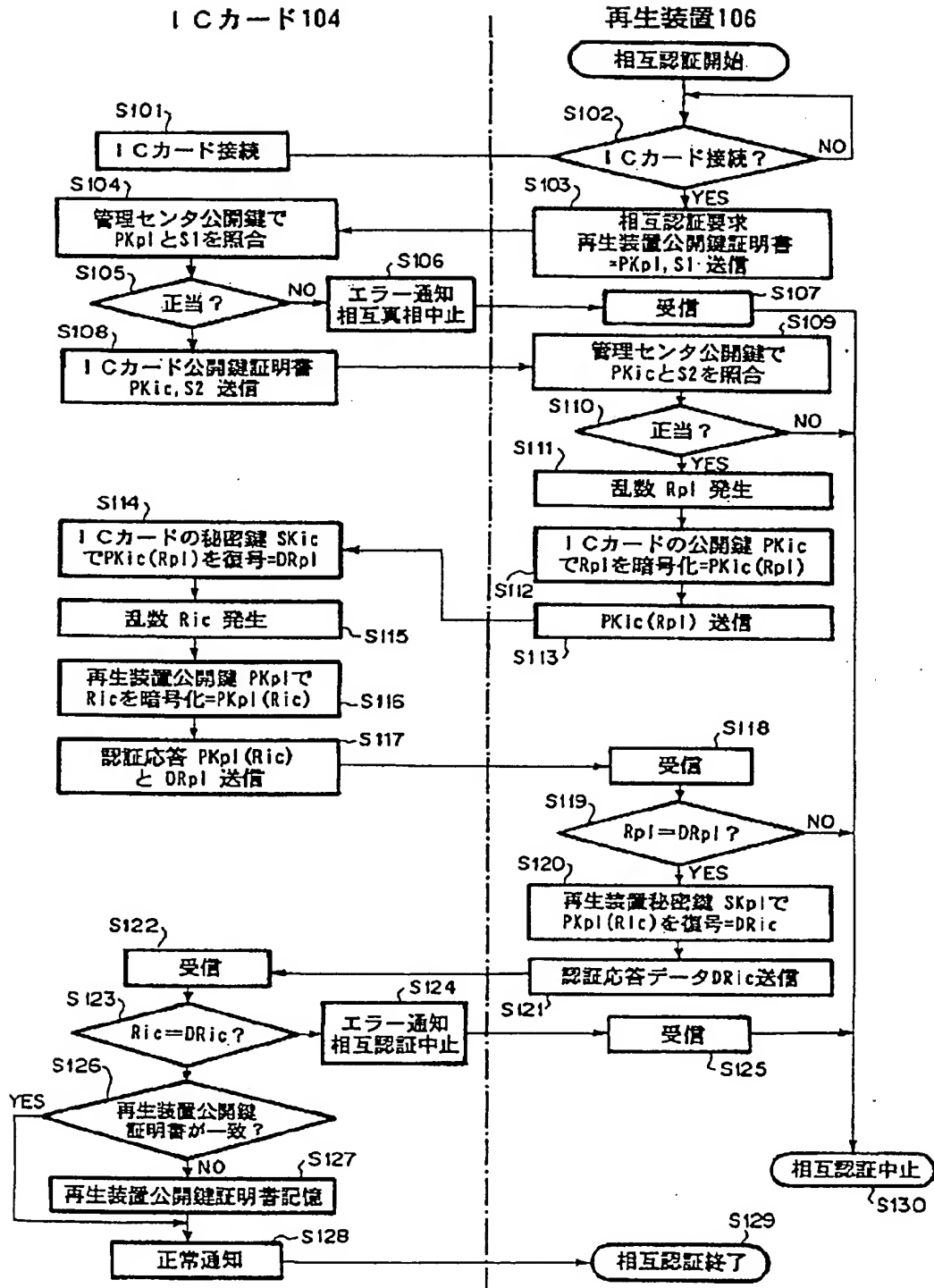
【図 4】



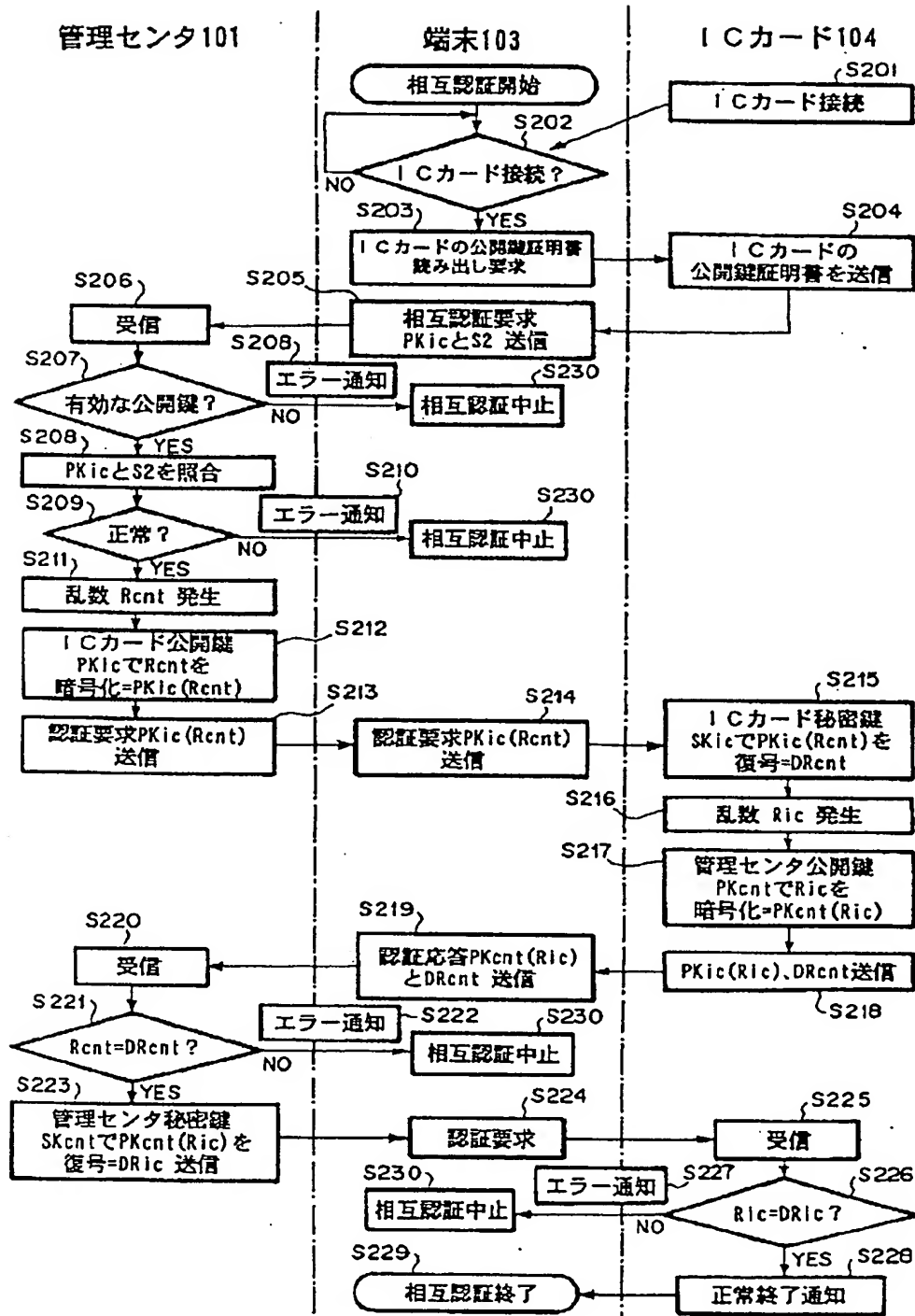
【図5】



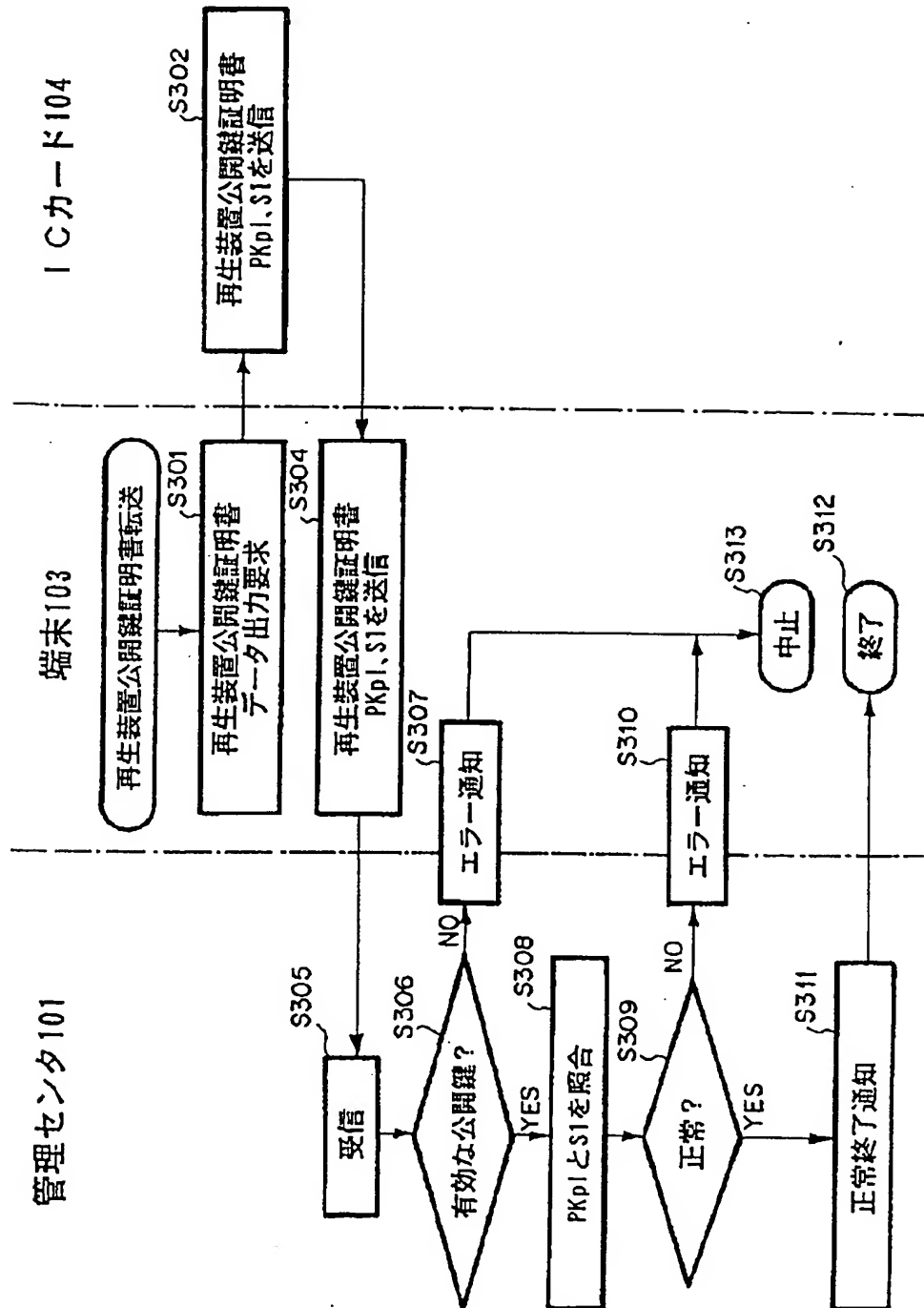
【図6】



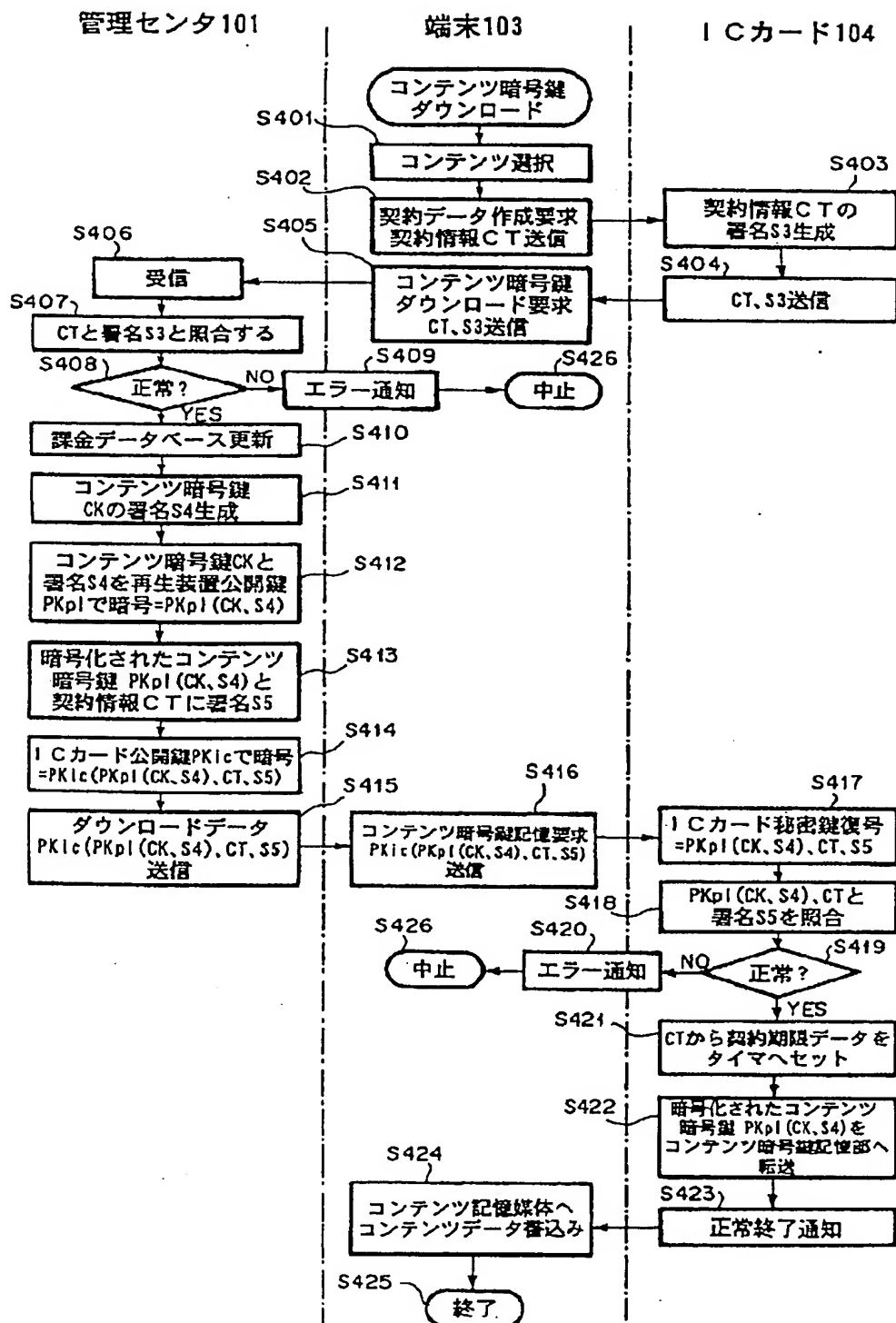
【図7】



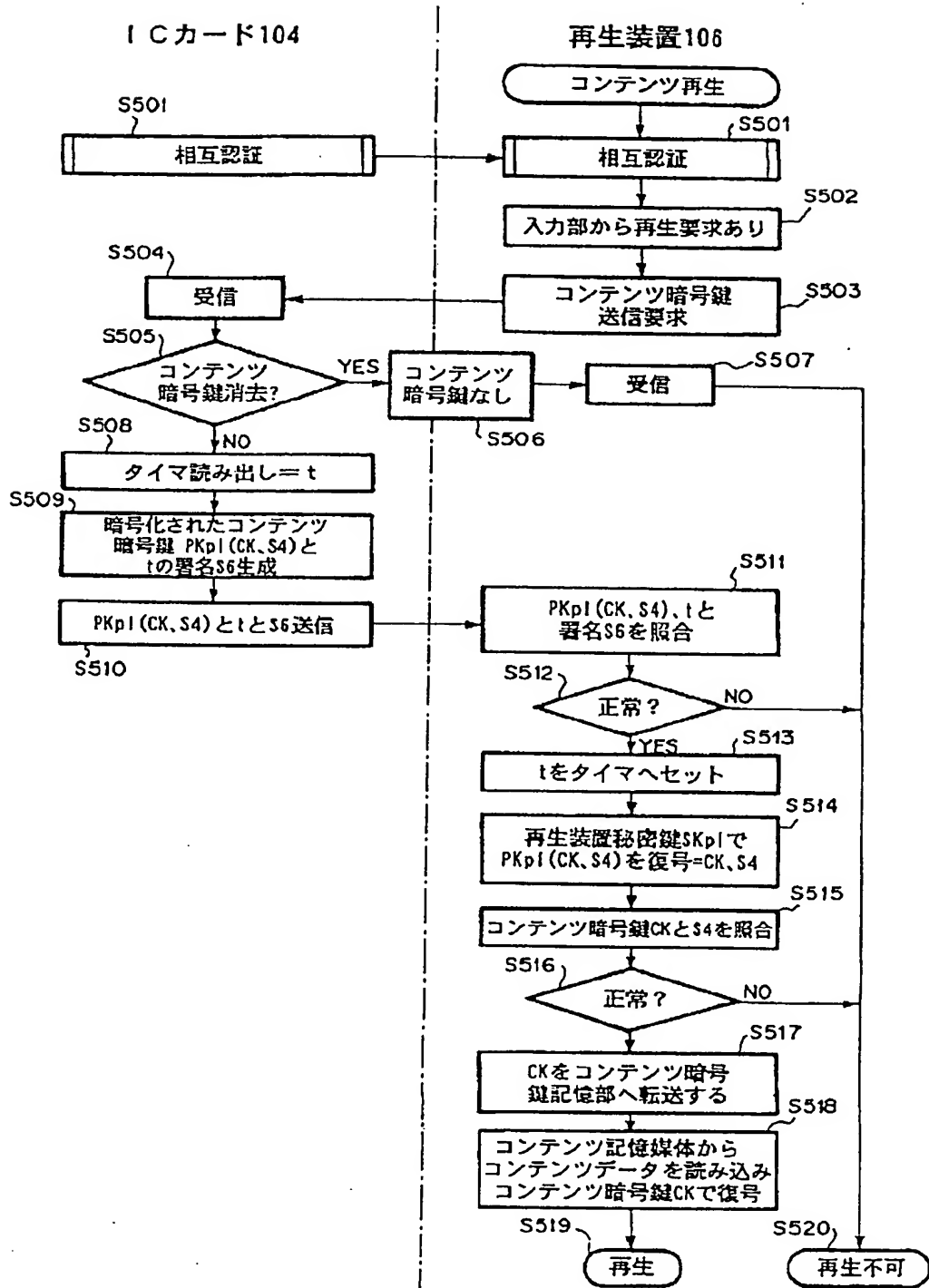
【図8】



【図9】



【図10】



フロントページの続き

| (51) Int. Cl. 7 | 識別記号 | F I | テ-マ-ド (参考) |
|---------------------|-------|---------------|--------------------------------|
| G 0 6 F 15/00 | 3 3 0 | G 0 6 F 15/00 | 3 3 0 Z 5 B 0 8 5 |
| 17/60 | Z E C | 17/60 | Z E C 5 J 1 0 4 |
| | 1 4 0 | | 1 4 0 |
| | 3 0 2 | | 3 0 2 E |
| | 3 4 2 | | 3 4 2 |
| | 5 1 0 | | 5 1 0 |
| G 0 6 K 17/00 | | G 0 6 K 17/00 | L |
| 19/00 | | 19/00 | T |
| 19/10 | | | Q |
| H 0 4 L 9/32 | | H 0 4 L 9/00 | R |
| | | | 6 7 5 B |
| | | | 6 7 5 D |
| (72) 発明者 塚本 雄二 | | F タ-ム (参考) | 5B017 AA03 BA05 BA07 BB10 CA16 |
| 東京都港区芝五丁目7番1号 日本電気株 | | | 5B035 AA15 BB09 BC00 CA29 |
| 式会社内 | | | 5B049 AA05 BB00 BB58 CC08 CC21 |
| (72) 発明者 菊地 芳秀 | | | DD01 DD04 EE01 EE23 EE28 |
| 東京都港区芝五丁目7番1号 日本電気株 | | | FF03 FF04 GG04 GG07 GG10 |
| 式会社内 | | | 5B058 CA27 KA02 KA04 KA13 KA33 |
| (72) 発明者 船矢 幸一 | | | KA35 YA20 |
| 東京都港区芝五丁目7番1号 日本電気株 | | | 5B082 EA12 GA02 GA12 |
| 式会社内 | | | 5B085 AA08 AC12 AE12 AE13 AE29 |
| (72) 発明者 大塚 修 | | | BE07 BG03 |
| 東京都港区芝五丁目7番1号 日本電気株 | | | 5J104 AA07 AA09 AA12 AA16 EA06 |
| 式会社内 | | | JA21 KA02 KA05 LA03 LA06 |
| | | | MA02 NA02 NA35 NA37 NA38 |
| | | | NA40 NA42 PA10 PA14 |